# 日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年　３月３０日

出 願 番 号
Application Number: 特願２０００－０９４３１３

出 願 人
Applicant (s): 株式会社日立製作所

２０００年１０月　６日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号　出証特２０００－３０８１６７１

【書類名】　特許願

【整理番号】　K00005401

【提出日】　平成12年 3月30日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 12/00

【発明者】

【住所又は居所】　東京都江東区新砂一丁目６番２７号　株式会社日立製作所　公共システム事業部内

【氏名】　篠田　隆志

【発明者】

【住所又は居所】　東京都江東区新砂一丁目６番２７号　株式会社日立製作所　公共システム事業部内

【氏名】　豊島　久

【発明者】

【住所又は居所】　東京都江東区新砂一丁目６番２７号　株式会社日立製作所　公共システム事業部内

【氏名】　中島　純三

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社日立製作所

【代理人】

【識別番号】　100083552

【弁理士】

【氏名又は名称】　秋田　収喜

【電話番号】　03-3893-6221

【手数料の表示】

【予納台帳番号】　014579

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コンテンツ改竄検知方法及びその実施装置並びにその処理プログラムを記録した記録媒体

【特許請求の範囲】

【請求項１】　コンテンツの改竄を検知するコンテンツ改竄検知方法において、

複数のコンテンツの現在の構成または内容に対応する改竄検知情報を生成するステップと、当該コンテンツの登録または更新時の構成または内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知するステップとを有することを特徴とするコンテンツ改竄検知方法。

【請求項２】　コンテンツの改竄を検知するコンテンツ改竄検知方法において、

あるコンテンツについて、その改竄を検知する為の改竄検知情報が生成済みであるかどうかを検査するステップと、当該コンテンツの改竄検知情報の有無を検査するステップとを有することを特徴とするコンテンツ改竄検知方法。

【請求項３】　コンテンツの改竄を検知するコンテンツ改竄検知方法において、

コンテンツの現在の内容に対応する改竄検知情報を生成するステップと、当該コンテンツの登録または更新時の内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知した場合に、当該コンテンツの要求元、登録元または更新元に通知するステップとを有することを特徴とするコンテンツ改竄検知方法。

【請求項４】　コンテンツの改竄を検知するコンテンツ改竄検知装置において、

複数のコンテンツの現在の構成または内容に対応する改竄検知情報を生成する改竄検知情報生成処理部と、当該コンテンツの登録または更新時の構成または内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知する改竄検知処理部とを備えることを特徴とするコンテンツ改竄検知装置。

【請求項５】　コンテンツの改竄を検知するコンテンツ改竄検知装置としてコンピュータを機能させる為のプログラムを記録したコンピュータ読み取り可能な記録媒体において、

複数のコンテンツの現在の構成または内容に対応する改竄検知情報を生成する改竄検知情報生成処理部と、当該コンテンツの登録または更新時の構成または内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知する改竄検知処理部としてコンピュータを機能させる為のプログラムを記録したことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はコンテンツの改竄を検知するコンテンツ改竄検知装置に関し、特にインターネットのホームページで表示されるコンテンツに対して行われた改竄を検知するコンテンツ改竄検知装置に適用して有効な技術に関するものである。

【０００２】

【従来の技術】

従来、個人を始め官公庁や多くの企業等がＷＷＷ(World Wide Web)サーバ装置にホームページを開設し、各種の情報発信を行っている。官公庁や企業が開設するホームページで公開される内容は、簡単なお知らせから公式な発表と同等な内容のものまで多岐に渡っており、インターネットにアクセスすることにより誰でもこれらの情報を得ることができる様になっている。

【０００３】

これらの官公庁や企業が開設するホームページの内容は、その官公庁や企業が外部に対して正式に発信しているものと考えられる為、その内容に誤りがあったり、外部の人間によるサーバへの不正侵入によりホームページの内容が改竄された場合、著しい信用の低下を招く場合がある。この為、簡単な広報活動の為にホームページを開設している場合であっても、そのセキュリティ対策を十分にとっておく必要があるが、近年では外部の人間が官公庁等のサーバに不正侵入し、ホームページの内容を改竄するという事件が相次いでいる。

【０００４】

なお厳密な電子データの真正性の認証を可能とすると共に、その真正性を視覚的に電子データの利用者に表現する認証可能な電子データの生成方法については、特開２０００－７８１２５号公報に記載されている。その概要は、Webページや商標などの電子マークＢを認証するための認証情報にデジタル署名を付加したものを、電子マークＡに不可視の電子透かしとして埋め込んだ後、真正性を視覚的に表現する電子マークＡを、電子マークＢに可視の電子透かしとして埋め込むものである。

【０００５】

【発明が解決しようとする課題】

前記の様なホームページの内容を改竄される事件での大きな問題は、ホームページを公開するサーバのセキュリティ対策が甘いということに加え、公開しているホームページの量が膨大である為、一部のホームページが改竄されてもそれに気付くのが遅れがちになるという点にある。

【０００６】

本発明の目的は上記問題を解決し、コンテンツの改竄を早期発見することが可能な技術を提供することにある。

【０００７】

本発明の他の目的は改竄検知情報の除去による改竄の隠蔽を防止することが可能な技術を提供することにある。

【０００８】

本発明の他の目的は改竄が行われた位置を特定することが可能な技術を提供することにある。

【０００９】

【課題を解決するための手段】

本発明は、コンテンツの改竄を検知するコンテンツ改竄検知装置において、複数のコンテンツの構成または内容の改竄を検知するものである。

【００１０】

本発明では、複数のコンテンツの登録または更新時にそれらの構成または内容

に対応する改竄検知情報を生成しておく。そして、所定の時刻になる等の所定の条件が成立した場合に、前記生成した改竄検知情報を参照し、当該コンテンツの現在の構成または内容に対応する改竄検知情報を生成した後、前記参照した改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知し、当該コンテンツの改竄を通知する。

【００１１】

例えば、公開しているホームページで表示される複数のコンテンツの登録または更新時に、それらのファイル構造や各ファイルの内容のハッシュ値を改竄検知情報として生成してＩＭ(Internet-Marks)に埋め込み、ホームページのトップページにそのＩＭを貼付しておく。

【００１２】

そして、常駐プログラム等の処理により所定の時刻になる等の所定の条件が成立した場合に、前記貼付したＩＭ中の登録または更新時のファイル構造や各ファイルの内容のハッシュ値を参照し、また現在のファイル構成や各ファイルの内容のハッシュ計算を行う。次に、前記参照したＩＭ中の登録または更新時のファイル構造や各ファイルの内容のハッシュ値と、前記生成した現在のファイル構造や各ファイルの内容のハッシュ値とを比較し、もし前記生成した現在のハッシュ値がＩＭに埋め込まれているハッシュ値と異なる場合は、システム管理者に通報すると共に、トップページのＩＭのデザインを変更してコンテンツの改竄が行われたことを閲覧者に知らせる。

【００１３】

前記の様に本発明では、システム管理者等の人間が常時チェックしなくても、公開しているホームページの一部が改竄された場合に、改竄が行われたことを即座に通知することが可能となり、不正の早期発見ができる。また同時に、閲覧者に対してもホームページの改竄が行われたことを即座に知らせることが可能となる。

【００１４】

以上の様に本発明のコンテンツ改竄検知装置によれば、複数のコンテンツの構成または内容の改竄を検知するので、コンテンツの改竄を早期発見することが可

能である。

【００１５】

【発明の実施の形態】

（実施形態１）

以下に複数のコンテンツの改竄を検知する実施形態１のコンテンツ改竄検知装置について説明する。

【００１６】

図１は本実施形態のコンテンツ改竄検知装置の概略構成を示す図である。図１に示す様に本実施形態のサーバ装置１００は、ＣＰＵ１０１と、メモリ１０２と、磁気ディスク装置１０３と、入力装置１０４と、出力装置１０５と、ＣＤ－ＲＯＭ装置１０６と、コンテンツデータ１０７と、ＩＭ１０８とを有している。

【００１７】

ＣＰＵ１０１は、サーバ装置１００全体の動作を制御する装置である。メモリ１０２は、サーバ装置１００全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。磁気ディスク装置１０３は、前記各種処理プログラムやデータを格納しておく記憶装置である。

【００１８】

入力装置１０４は、複数のコンテンツの改竄を検知する為の各種入力を行う装置である。出力装置１０５は、複数のコンテンツの改竄の検知に伴う各種出力を行う装置である。ＣＤ－ＲＯＭ装置１０６は、前記各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。

【００１９】

コンテンツデータ１０７は、クライアント装置１２０からの要求に応じて公開されるページの内容を示すデータである。ＩＭ１０８は、複数のコンテンツデータ１０７に対応する改竄検知情報を埋め込んだ画像データである。

【００２０】

またサーバ装置１００は、ＩＭ生成処理部１１０と、改竄検知情報生成処理部１１１と、改竄検知処理部１１２とを有している。

【００２１】

ＩＭ生成処理部１１０は、複数のコンテンツの登録または更新時の構成または内容に対応する改竄検知情報を埋め込んだＩＭを生成する処理部である。改竄検知情報生成処理部１１１は、複数のコンテンツの構成または内容に対応する改竄検知情報を生成する処理部である。

【００２２】

改竄検知処理部１１２は、複数のコンテンツの登録または更新時の構成または内容に対応する改竄検知情報と、当該コンテンツの現在の構成または内容に対応する改竄検知情報とを比較して当該コンテンツの改竄を検知する処理部である。

【００２３】

サーバ装置１００をＩＭ生成処理部１１０、改竄検知情報生成処理部１１１及び改竄検知処理部１１２として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。

【００２４】

コンテンツデータを管理・公開するサーバ装置１００と、コンテンツデータを閲覧するクライアント装置１２０は、インターネット等のネットワークにより相互にデータの送受信が可能であるものとする。

【００２５】

サーバ装置１００には、クライアント装置１２０からの要求に応じてコンテンツデータの公開を行うＷＷＷサーバが実装され、クライアント装置１２０には、サーバ装置からコンテンツデータを受信し、表示するＷＷＷブラウザが実装される。

【００２６】

また、サーバ装置１００に接続される磁気ディスク装置１０３には、複数のコンテンツデータ１０７を格納し、そのうちの１つ、例えばコンテンツのトップページに、複数のコンテンツデータ１０７に対応する改竄検知情報を埋め込んだインターネットマークであるＩＭ１０８を貼付することとする。

【００２７】

図２は本実施形態のＩＭ生成処理部１１０の処理手順を示すフローチャートである。図２に示す様にサーバ装置１００のＩＭ生成処理部１１０は、複数のコンテンツの登録または更新時の構成または内容に対応する改竄検知情報を埋め込んだＩＭを生成する処理を行う。

【００２８】

ステップ２０１でＩＭ生成処理部１１０は、複数のコンテンツの構成に対応する改竄検知情報として、複数のコンテンツを構成する各コンテンツのパス名（ディレクトリ名）を含むファイル名に対応したハッシュ値を改竄検知情報生成処理部１１１により生成し、ステップ２０２では、ステップ２０１で生成した改竄検知情報をＩＭ１０８に埋め込む。

【００２９】

ステップ２０３でＩＭ生成処理部１１０は、複数のコンテンツの内容に対応する改竄検知情報として、複数のコンテンツを構成する各コンテンツデータ１０７の内容に対応したハッシュ値を改竄検知情報生成処理部１１１により生成する。ステップ２０４では、ステップ２０３で生成した改竄検知情報をＩＭ１０８に埋め込み、前記の様に複数のコンテンツの改竄検知情報が埋め込まれたＩＭ１０８をトップページに貼付ける。

【００３０】

図３は本実施形態のパス名を含むファイル名に対応したハッシュ値の生成処理の概要を示す図である。図３に示す様にステップ２０１の処理では、改竄検知情報生成の対象となるコンテンツデータ１０７のパス名付きのファイル名３００を取得し、取得したファイル名３００の並びが一意に決定する様、取得したファイル名３００をアルファベット順等でソートした後、それらのファイル名３００のデータを連結してハッシュ値３２０を計算する。

【００３１】

図４は本実施形態のパス名を含むファイル名に対応したハッシュ値の生成処理の処理手順を示すフローチャートである。図４に示す様にサーバ装置１００の改竄検知情報生成処理部１１１は、複数のコンテンツのパス名を含むファイル名に対応する改竄検知情報を生成する処理を行う。

【００３２】

ステップ４０１で改竄検知情報生成処理部１１１は、改竄検知情報の生成の対象となるコンテンツを選択し、そのコンテンツデータ１０７のパス名付きのファイル名３００を取得する。例えばサーバ装置１００で公開しているホームページのトップページ以下に存在しているＨＴＭＬ(Hyper Text Markup Language)やＸＭＬ(eXtensible Markup Language)等のＷｅｂページを記述する為の記述言語で記載されたファイルやそれらのファイルにより表示される画像ファイルを選択したり、またトップページからリンクしているページの内でサーバ装置１００内に存在しているページのファイルそれらのファイルにより表示される画像ファイルを選択する。また改竄検知情報を生成するファイルを定義した生成情報を別途作成し、この生成情報に従ってサーバ装置１００中の特定のファイルについてのみ改竄検知情報を生成するものとしても良い。

【００３３】

ステップ４０２では、ステップ４０１で取得したファイル名３００の並びが一意に決定する様、取得したファイル名３００をアルファベット順等でソートする。そしてステップ４０３では、それらのファイル名３００のデータを連結し、ステップ４０４では、前記連結したファイル名３００のデータについてのハッシュ値３２０を計算する。

【００３４】

図５は本実施形態のコンテンツの内容に対応したハッシュ値の生成処理の概要を示す図である。図５に示す様にステップ２０３の処理では、先程取得したファイル名３１０のそれぞれについて、対応する実際のコンテンツデータ５００を取得する。更に、各コンテンツデータのハッシュ値５１０を計算する。次に、それらのハッシュ値５１０を連結し、それについてのハッシュ値５２０を計算する。

【００３５】

図６は本実施形態のコンテンツの内容に対応したハッシュ値の生成処理の処理手順を示すフローチャートである。図６に示す様にサーバ装置１００の改竄検知情報生成処理部１１１は、複数のコンテンツのコンテンツデータに対応する改竄検知情報を生成する処理を行う。

【００３６】

ステップ６０１で改竄検知情報生成処理部１１１は、先程取得したファイル名３１０のそれぞれについて、対応する実際のコンテンツデータ５００を取得し、ステップ６０２では、各コンテンツデータ５００のハッシュ値５１０を計算する。

【００３７】

ステップ６０３では、各コンテンツデータ５００のハッシュ値５１０を連結し、ステップ６０４では、前記連結したハッシュ値５１０についてのハッシュ値５２０を計算する。

【００３８】

前記の様にＩＭ１０８に埋め込んむファイル名３００のハッシュ値３２０及びコンテンツデータ５００のハッシュ値５２０は、コンテンツの改竄を検知する時に、正しい値として使用するものである。従って、コンテンツデータ５００の内容やファイル構成を変更した場合は、その都度、上記の通り各々のハッシュ値を計算し、ＩＭ１０８に埋め込み直す必要がある。但し、コンテンツデータ５００が変更される都度、ＩＭ１０８を自動生成し、コンテンツデータ５００に自動貼付するようなジェネレータを用意することで、利用者の操作を不要とすることも可能である。

【００３９】

図７は本実施形態の改竄検知処理部１１２の処理手順を示すフローチャートである。図７に示す様にサーバ装置１００の改竄検知処理部１１２は、複数のコンテンツの登録または更新時の構成または内容に対応する改竄検知情報と、当該コンテンツの現在の構成または内容に対応する改竄検知情報とを比較して当該コンテンツの改竄を検知する処理を行う。

【００４０】

ステップ７０１で改竄検知処理部１１２は、図４に示した処理と同様にして複数のコンテンツを構成する各コンテンツについてそれらのパス名を含むファイル名に対するハッシュ値を改竄検知情報生成処理部１１１により計算する。

【００４１】

ステップ７０２では、ＩＭ１０８内に埋め込まれているハッシュ値３２０と前記計算したハッシュ値の値とを比較し、ＩＭ１０８内に埋め込まれているハッシュ値３２０が前記計算したハッシュ値と異なる場合にはステップ７０３へ進む。

【００４２】

前記パス名を含むファイル名に対するハッシュ値の相違は、コンテンツデータ１０７のファイル構成の改竄(コンテンツデータ１０７の削除・追加等)が行われたことを表している。従ってステップ７０３では、ファイル構成の改竄が行われたことを示す改竄通告を行う。改竄通告の方法としては、例えばシステム管理者のコンソール画面にメッセージを表示したり、或いは閲覧者がコンテンツのトップページを参照した時、ＩＭ１０８の画像デザインを変更し、コンテンツの改竄がなされていることを示す等が考えられる。

【００４３】

ステップ７０４では、図６で示した処理と同様にして複数のコンテンツを構成する各コンテンツについてそれらの各コンテンツデータ５００に対するハッシュ値を改竄検知情報生成処理部１１１により計算する。

【００４４】

ステップ７０５では、ＩＭ１０８内に埋め込まれているハッシュ値５２０と前記計算したハッシュ値の値とを比較し、ＩＭ１０８内に埋め込まれているハッシュ値５２０が前記計算したハッシュ値と異なる場合にはステップ７０６へ進む。

【００４５】

前記各コンテンツデータ５００に対するハッシュ値の相違は、コンテンツデータ５００のファイル内容の改竄(コンテンツの文章の一部変更等)が行われたことを表している。従って、ステップ７０６では、ファイル内容の改竄が行われたことを示す改竄通告を行う。

【００４６】

本実施形態では、改竄を検知する為の元データとして、パス付きのファイル名及び実際のコンテンツデータを用いているが、これらに加え、ファイル属性、コンテンツに貼付されている各種データ、リンクされている他のコンテンツ等を含めても良い。また、改竄を検知する為の情報として、ディレクトリやファイルの

更新日時等を用いても良い。

【００４７】

本実施形態では、改竄検知情報としてハッシュ値を計算し、ＩＭに埋め込んでいるが、これはデータの容量を少なく抑えることが目的である。従ってハッシュ値を計算せず、パス付きファイル名のデータや各コンテンツデータをそのままＩＭに埋め込んでも良い。また、各コンテンツデータ５００のハッシュ値５１０をそのままＩＭに埋め込んだり、各コンテンツデータ５００を連結し、それに対して計算したハッシュ値をＩＭに埋め込む形態も可能である（コンテンツデータを特定する情報が残る形態であれば良い）。

【００４８】

本実施形態では、改竄検知情報をトップページのＩＭに格納したが、各コンテンツ毎にＩＭを貼付しても良い。また、改竄検知情報をＩＭに埋め込むのではなく、デジタル署名としたり或いは加工せずにそのままの状態で磁気ディスク装置１０３内に格納しても良い。

【００４９】

本実施形態において改竄検知処理部１１２を起動させる際には、サーバ装置１００の管理者等の手により手動で起動させる以外に、定期的に自動起動させたり、メモリに常駐させて常時検知を行ったり、また、閲覧者がコンテンツデータを参照した時に自動起動させる等の処理を行っても良い。

【００５０】

以上説明した様に本実施形態のコンテンツ改竄検知装置によれば、複数のコンテンツの構成または内容の改竄を検知するので、コンテンツの改竄を早期発見することが可能である。

（実施形態２）

以下にＥＸＩＴゲートを用いて改竄検知情報の有無を検知すると共に改竄位置を特定する実施形態２のコンテンツ改竄検知装置について説明する。

【００５１】

図８は本実施形態のコンテンツ改竄検知装置の概要を示す図である。図８に示す様に本実施形態の改竄検知システムは、サーバ装置８００と、ＥＸＩＴゲート

装置８１０と、クライアント装置８２０とを有している。

【００５２】

サーバ装置８００は、コンテンツの登録または更新時の内容に対応する改竄検知情報を埋め込んだＩＭを貼付してコンテンツを生成し、ＥＸＩＴゲート装置８１０を介してクライアント装置８２０へ当該コンテンツを送信する装置である。

【００５３】

ＥＸＩＴゲート装置８１０は、クライアント装置８２０から要求されたコンテンツの改竄を検知する装置である。クライアント装置８２０は、ＥＸＩＴゲート装置８１０から受け取ったコンテンツの改竄を検知し、改竄の行われていないコンテンツを表示する装置である。

【００５４】

図８に示す様に本実施形態では、サーバ装置８００とクライアント装置８２０との間にＥＸＩＴゲート装置８１０を設け、ＥＸＩＴゲート装置８１０にてＩＭの有無のチェックやＩＭを用いた改竄検知を行う。またクライアント装置８２０でのチェックを併用することにより、サーバ装置８００上またはサーバ装置８００からＥＸＩＴゲート装置８１０までの経路上、若しくはＥＸＩＴゲート装置８１０からクライアント装置８２０までの経路上で改竄が行われているかどうかをチェックする。

【００５５】

図９は本実施形態のサーバ装置８００の概略構成を示す図である。図９に示す様に本実施形態のサーバ装置８００は、ＣＰＵ９０１と、メモリ９０２と、磁気ディスク装置９０３と、入力装置９０４と、出力装置９０５と、ＣＤ－ＲＯＭ装置９０６と、コンテンツデータ９０７と、ＩＭ９０８と、生成情報９０９とを有している。

【００５６】

ＣＰＵ９０１は、サーバ装置８００全体の動作を制御する装置である。メモリ９０２は、サーバ装置８００全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。磁気ディスク装置９０３は、前記各種処理プログラムやデータを格納しておく記憶装置である。

【００５７】

入力装置９０４は、コンテンツを登録したり更新する為の各種入力を行う装置である。出力装置９０５は、コンテンツの登録や更新に伴う各種出力を行う装置である。ＣＤ－ＲＯＭ装置９０６は、前記各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。

【００５８】

コンテンツデータ９０７は、クライアント装置１２０からの要求に応じて公開されるページの内容を示すデータである。ＩＭ９０８は、コンテンツデータ９０７に対応する改竄検知情報を埋め込んだ画像データである。生成情報９０９は、コンテンツの改竄を検知する為の改竄検知情報が生成されたコンテンツを示すデータである。

【００５９】

またサーバ装置８００は、ＩＭ生成処理部９１０と、改竄検知情報生成処理部９１１と、生成情報作成処理部９１２と、改竄通知受信処理部９１３とを有している。

【００６０】

ＩＭ生成処理部９１０は、コンテンツの内容に対応する改竄検知情報を埋め込んだＩＭ９０８を生成する処理部である。改竄検知情報生成処理部９１１は、コンテンツの内容に対応する改竄検知情報を生成する処理部である。

【００６１】

生成情報作成処理部９１２は、コンテンツの改竄を検知する為の改竄検知情報が生成されたコンテンツを示す生成情報９０９を作成する処理部である。改竄通知受信処理部９１３は、コンテンツの改竄が行われていることを示す通知をＥＸＩＴゲート装置８１０から受信する処理部である。

【００６２】

サーバ装置８００をＩＭ生成処理部９１０、改竄検知情報生成処理部９１１、生成情報作成処理部９１２及び改竄通知受信処理部９１３として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録

する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。

【００６３】

図１０は本実施形態のＥＸＩＴゲート装置８１０の概略構成を示す図である。図１０に示す様に本実施形態のＥＸＩＴゲート装置８１０は、ＣＰＵ１００１と、メモリ１００２と、磁気ディスク装置１００３と、入力装置１００４と、出力装置１００５と、ＣＤ－ＲＯＭ装置１００６とを有している。

【００６４】

ＣＰＵ１００１は、ＥＸＩＴゲート装置８１０全体の動作を制御する装置である。メモリ１００２は、ＥＸＩＴゲート装置８１０全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。

【００６５】

磁気ディスク装置１００３は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置１００４は、コンテンツの改竄を検知する為の各種入力を行う装置である。出力装置１００５は、コンテンツの改竄の検知に伴う各種出力を行う装置である。ＣＤ－ＲＯＭ装置１００６は、前記各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。

【００６６】

またＥＸＩＴゲート装置８１０は、生成検査処理部１０１０と、存在検査処理部１０１１と、改竄検知情報生成処理部１０１２と、改竄検知処理部１０１３とを有している。

【００６７】

生成検査処理部１０１０は、コンテンツの改竄を検知する為の改竄検知情報が生成されたコンテンツを示す生成情報９０９を参照し、クライアント装置８２０から要求されたコンテンツについて、その改竄を検知する為の改竄検知情報が生成済みであるかどうかを検査する処理部である。

【００６８】

存在検査処理部１０１１は、クライアント装置８２０から要求されたコンテンツについて、そのコンテンツの改竄検知情報の有無を検査する処理部である。改竄検知情報生成処理部１０１２は、クライアント装置８２０から要求されたコン

テンツの現在の内容に対応する改竄検知情報を生成する処理部である。

【００６９】

改竄検知処理部１０１３は、当該コンテンツの登録または更新時の内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知した場合に、サーバ装置８００上またはサーバ装置８００からＥＸＩＴゲート装置８１０までの経路上での当該コンテンツの改竄を検知したことを当該コンテンツの要求元であるクライアント装置８２０、登録元及び更新元であるサーバ装置８００に通知する処理部である。

【００７０】

ＥＸＩＴゲート装置８１０を生成検査処理部１０１０、存在検査処理部１０１１、改竄検知情報生成処理部１０１２及び改竄検知処理部１０１３として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。

【００７１】

図１１は本実施形態のクライアント装置８２０の概略構成を示す図である。図１１に示す様に本実施形態のクライアント装置８２０は、ＣＰＵ１１０１と、メモリ１１０２と、磁気ディスク装置１１０３と、入力装置１１０４と、出力装置１１０５と、ＣＤ－ＲＯＭ装置１１０６とを有している。

【００７２】

ＣＰＵ１１０１は、クライアント装置８２０全体の動作を制御する装置である。メモリ１１０２は、クライアント装置８２０全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。

【００７３】

磁気ディスク装置１１０３は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置１１０４は、コンテンツを要求して表示する為の各種入力を行う装置である。出力装置１１０５は、コンテンツの要求に伴ってコンテンツを表示する装置である。ＣＤ－ＲＯＭ装置１１０６は、前記各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。

【００７４】

またクライアント装置８２０は、改竄検知情報生成処理部１１１０と、改竄検知処理部１１１１とを有している。

【００７５】

改竄検知情報生成処理部１１１０は、要求したコンテンツをＥＸＩＴゲート装置８１０から受け取り、そのコンテンツの現在の内容に対応する改竄検知情報を生成する処理部である。改竄検知処理部１１１１は、当該コンテンツの登録または更新時の内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知した場合に、ＥＸＩＴゲート装置８１０からクライアント装置８２０までの経路上での当該コンテンツの改竄を検知したことを示す表示を行う処理部である。

【００７６】

クライアント装置８２０を改竄検知情報生成処理部１１１０及び改竄検知処理部１１１１として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。

【００７７】

図１２は本実施形態のコンテンツ登録／更新処理の処理手順を示すフローチャートである。図１２に示す様にサーバ装置８００では、登録や更新が行われたコンテンツの内容に対応する改竄検知情報を埋め込んだＩＭ９０８を生成して当該コンテンツに貼付けた後、ＩＭ９０８の貼付けが行われたコンテンツを示す生成情報９０９を作成する処理を行う。

【００７８】

ステップ１２０１でＩＭ生成処理部９１０は、コンテンツデータ９０７の登録や更新が行われたかどうかを調べ、コンテンツデータ９０７の登録や更新が行われている場合にはステップ１２０２へ進む。

【００７９】

ステップ１２０２では、登録や更新が行われたコンテンツについて、そのコン

テンツデータ９０７のハッシュ値を改竄検知情報生成処理部９１１により計算し、その内容に対応する改竄検知情報としてＩＭ９０８に埋め込む。そしてステップ１２０３では、ステップ１２０２で改竄検知情報を埋め込んだＩＭ９０８を、前記登録や更新が行われたコンテンツに貼付ける。

【００８０】

ステップ１２０４で生成情報作成処理部９１２は、ステップ１２０３でＩＭ９０８の貼付けが行われたコンテンツを示す情報を生成情報９０９に設定し、ステップ１２０５では、前記設定した生成情報９０９をＥＸＩＴゲート装置８１０へ送る。

【００８１】

図１３は本実施形態の生成情報９０９の一例を示す図である。図１３に示す様に生成情報９０９には、ＩＭ９０８の貼付けが行われたコンテンツを示す情報として、ＩＭ９０８の貼付けが行われたコンテンツデータ９０７のパス名を含むファイル名や貼付けられたＩＭ９０８の生成日付時刻等の情報が設定されている。

【００８２】

図１４は本実施形態のクライアント側処理の処理手順を示すフローチャートである。図１４に示す様にクライアント装置８２０は、要求したコンテンツをＥＸＩＴゲート装置８１０から受け取り、そのコンテンツの現在の内容に対応する改竄検知情報を生成して改竄を検知する処理を行う。

【００８３】

ステップ１４０１でクライアント装置８２０のWWWブラウザは、ユーザがＵＲＬ(Uniform Resource Locators)を入力したかどうかを調べ、ユーザがＵＲＬを入力した場合にはそのＵＲＬを受付けてステップ１４０２へ進む。ステップ１４０２では、ステップ１４０１で受付けたＵＲＬのページを表示する為のリクエストを前記ＵＲＬで示される宛先へ送信する。前記ＵＲＬで示される宛先がサーバ装置８００であり、その経路上にＥＸＩＴゲート装置８１０がある場合には、前記リクエストはＥＸＩＴゲート装置８１０を経由してサーバ装置８００へ送られる。

【００８４】

ステップ１４０３では、前記送信したリクエストの結果としてＨＴＭＬデータを受信しているかどうかを調べ、ＨＴＭＬデータを受信している場合にはステップ１４０４へ進む。

【００８５】

ステップ１４０４では、ステップ１４０３で受信したＨＴＭＬデータ中にＩＭ９０８が貼付けられているかどうかを調べ、ＩＭ９０８が貼付けられている場合にはステップ１４０５へ進み、ＩＭ９０８が貼付けられていない場合にはステップ１４０６へ進む。

【００８６】

ステップ１４０５で改竄検知処理部１１１１は、ステップ１４０３で受信したＨＴＭＬデータについて、その内容に対するハッシュ値を改竄検知情報生成処理部１１１０により計算し、ＩＭ９０８中のハッシュ値と前記計算したハッシュ値とを比較して当該コンテンツの改竄が行われているかどうかを調べる。当該コンテンツの改竄が行われているかどうかを調べた結果、当該コンテンツの改竄が検知されない場合にはステップ１４０６へ進み、当該コンテンツの改竄を検知した場合にはステップ１４０７へ進む。

【００８７】

ステップ１４０６では、ステップ１４０３で受信したＨＴＭＬデータに従ってページを表示する。ここで前記ＵＲＬのリクエストを処理する際にＥＸＩＴゲート装置８１０が当該ページの改竄を検知した場合には、改竄が検知されたことを示すＨＴＭＬデータがＥＸＩＴゲート装置８１０から送られてきているので、クライアント装置８２０では当該ページの改竄がＥＸＩＴゲート装置８１０で検知されたことを示す表示が行われる。

【００８８】

ステップ１４０７では、ステップ１４０３で受信したＨＴＭＬデータ中にＥＸＩＴゲート装置８１０での処理が行われたことを示す情報が含まれているかを調べ、ＥＸＩＴゲート装置８１０での処理が行われたことを示す情報が含まれている場合にはステップ１４０８へ進み、含まれていない場合にはステップ１４０９へ進む。

【００８９】

ステップ１４０８では、ＥＸＩＴゲート装置８１０からクライアント装置８２０までの経路上での当該コンテンツの改竄を検知したことを示す表示を行い、ステップ１４０９では、単に当該コンテンツの改竄を検知したことを示す表示を行う。

【００９０】

図１５は本実施形態のＥＸＩＴゲート側処理の処理手順を示すフローチャートである。ステップ１５０１でＥＸＩＴゲート装置８１０の改竄検知処理部１０１３は、クライアント装置８２０からリクエストを受信しているかどうかを調べ、リクエストを受信している場合にはステップ１５０２へ進む。

【００９１】

ステップ１５０２では、当該リクエストで要求されているコンテンツデータ９０７をキャッシュとして保持しているかどうかを調べ、保持していない場合にはステップ１５０３で当該リクエストをサーバ装置８００へ送る。

【００９２】

ステップ１５０４では、当該リクエストに対応するＨＴＭＬデータをサーバ装置８００から受信しているかどうかを調べ、ＨＴＭＬデータを受信している場合にはステップ１５０５へ進む。

【００９３】

ステップ１５０５で生成検査処理部１０１０は、コンテンツの改竄を検知する為の改竄検知情報が生成されたコンテンツを示す生成情報９０９を参照する。ステップ１５０６では、クライアント装置８２０から要求されたコンテンツについて、その改竄を検知する為の改竄検知情報が生成済みであるかどうかを調べ、改竄検知情報が生成済みである場合にはステップ１５０７へ進む。

【００９４】

ステップ１５０７で存在検査処理部１０１１は、ステップ１５０４で受信したＨＴＭＬデータ中に生成情報９０９で示されたＩＭ９０８が貼付けられているかどうかを調べ、クライアント装置８２０から要求されたコンテンツについて、そのコンテンツの改竄検知情報の有無を検査する処理を行う。生成情報９０９で示

されたＩＭ９０８が貼付けられている場合にはステップ１５０８へ進み、生成情報９０９で示されたＩＭ９０８が貼付けられていない場合にはステップ１５１１へ進む。

【００９５】

ステップ１５０８で改竄検知処理部１０１３は、ステップ１５０４で受信したＨＴＭＬデータについて、その内容に対するハッシュ値を改竄検知情報生成処理部１０１２により計算し、ＩＭ９０８中のハッシュ値と前記計算したハッシュ値とを比較して当該コンテンツの改竄が行われているかどうかを調べる。当該コンテンツの改竄が行われているかどうかを調べた結果、当該コンテンツの改竄が検知されない場合にはステップ１５０９へ進み、当該コンテンツの改竄を検知した場合にはステップ１５１２へ進む。

【００９６】

ステップ１５０９では、ステップ１５０４で受信したＨＴＭＬデータであるコンテンツデータ９０７をキャッシュとして保持し、ステップ１５１０では、ＥＸＩＴゲート装置８１０での処理が行われたことを示す情報と共に当該ＨＴＭＬデータをクライアント装置８２０へ送信する。

【００９７】

ステップ１５１１では、サーバ装置８００上またはサーバ装置８００からＥＸＩＴゲート装置８１０までの経路上での当該コンテンツの改竄検知情報の除去を検知したことを示す表示を行う。またステップ１５１２では、サーバ装置８００上またはサーバ装置８００からＥＸＩＴゲート装置８１０までの経路上での当該コンテンツの内容の改竄を検知したことを示す表示を行う。

【００９８】

ステップ１５１３では、当該コンテンツの登録元及び更新元であるサーバ装置８００に、サーバ装置８００上またはサーバ装置８００からＥＸＩＴゲート装置８１０までの経路上で、当該コンテンツの改竄検知情報の除去または当該コンテンツの内容の改竄が行われたことを通知する処理を行う。

【００９９】

またステップ１５１３では、当該コンテンツの要求元であるクライアント装置

８２０に、サーバ装置８００上またはサーバ装置８００からＥＸＩＴゲート装置８１０までの経路上で、当該コンテンツの改竄検知情報の除去または当該コンテンツの内容の改竄が行われたことを通知する処理を行う。

【０１００】

図１６は本実施形態の改竄通知受信処理部９１３の処理手順を示すフローチャートである。図１６に示す様にサーバ装置８００の改竄通知受信処理部９１３は、コンテンツの改竄が行われていることを示す通知をＥＸＩＴゲート装置８１０から受信する処理を行う。

【０１０１】

ステップ１６０１で改竄通知受信処理部９１３は、コンテンツの改竄が行われていることを示す通知をＥＸＩＴゲート装置８１０から受信しているかどうかを調べ、コンテンツの改竄が行われていることを示す通知を受信している場合にはステップ１６０２へ進む。ステップ１６０２では、受信した通知内容を表示してサーバ装置８００の管理者に知らせ、ステップ１６０３では、受信した通知内容を磁気ディスク装置９０３に格納する。

【０１０２】

以上説明した様に本実施形態のコンテンツ改竄検知装置によれば、改竄検知情報の有無を検査するので、改竄検知情報の除去による改竄の隠蔽を防止することが可能である。

【０１０３】

また本実施形態のコンテンツ改竄検知装置によれば、クライアントとサーバの間でコンテンツの改竄を検知するので、改竄が行われた位置を特定することが可能である。

【０１０４】

【発明の効果】

本発明によれば複数のコンテンツの構成または内容の改竄を検知するので、コンテンツの改竄を早期発見することが可能である。

【図面の簡単な説明】

【図１】

実施形態１のコンテンツ改竄検知装置の概略構成を示す図である。

【図２】

実施形態１のＩＭ生成処理部１１０の処理手順を示すフローチャートである。

【図３】

実施形態１のパス名を含むファイル名に対応したハッシュ値の生成処理の概要を示す図である。

【図４】

実施形態１のパス名を含むファイル名に対応したハッシュ値の生成処理の処理手順を示すフローチャートである。

【図５】

実施形態１のコンテンツの内容に対応したハッシュ値の生成処理の概要を示す図である。

【図６】

実施形態１のコンテンツの内容に対応したハッシュ値の生成処理の処理手順を示すフローチャートである。

【図７】

実施形態１の改竄検知処理部１１２の処理手順を示すフローチャートである。

【図８】

実施形態２のコンテンツ改竄検知装置の概要を示す図である。

【図９】

実施形態２のサーバ装置８００の概略構成を示す図である。

【図１０】

実施形態２のＥＸＩＴゲート装置８１０の概略構成を示す図である。

【図１１】

実施形態２のクライアント装置８２０の概略構成を示す図である。

【図１２】

実施形態２のコンテンツ登録／更新処理の処理手順を示すフローチャートである。

【図１３】

実施形態２の生成情報９０９の一例を示す図である。

【図１４】

実施形態２のクライアント側処理の処理手順を示すフローチャートである。

【図１５】

実施形態２のＥＸＩＴゲート側処理の処理手順を示すフローチャートである。

【図１６】

実施形態２の改竄通知受信処理部９１３の処理手順を示すフローチャートである。

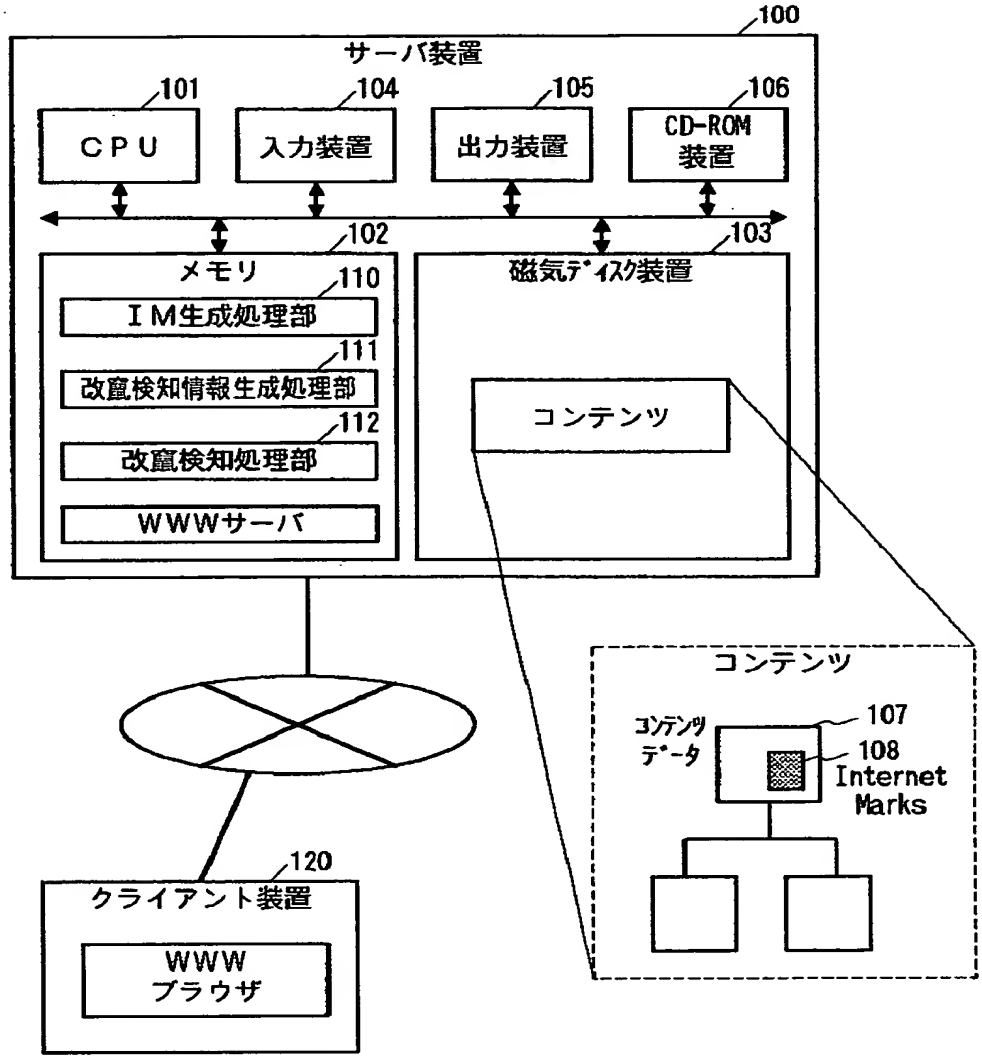
【符号の説明】

１００…サーバ装置、１２０…クライアント装置、１０１…ＣＰＵ、１０２…メモリ、１０３…磁気ディスク装置、１０４…入力装置、１０５…出力装置、１０６…ＣＤ－ＲＯＭ装置、１０７…コンテンツデータ、１０８…ＩＭ、１１０…ＩＭ生成処理部、１１１…改竄検知情報生成処理部、１１２…改竄検知処理部、３００及び３１０…ファイル名、３２０…ハッシュ値、５００…コンテンツデータ、５１０及び５２０…ハッシュ値、８００…サーバ装置、８１０…ＥＸＩＴゲート装置、８２０…クライアント装置、９０１…ＣＰＵ、９０２…メモリ、９０３…磁気ディスク装置、９０４…入力装置、９０５…出力装置、９０６…ＣＤ－ＲＯＭ装置、９０７…コンテンツデータ、９０８…ＩＭ、９０９…生成情報、９１０…ＩＭ生成処理部、９１１…改竄検知情報生成処理部、９１２…生成情報作成処理部、９１３…改竄通知受信処理部、１００１…ＣＰＵ、１００２…メモリ、１００３…磁気ディスク装置、１００４…入力装置、１００５…出力装置、１００６…ＣＤ－ＲＯＭ装置、１０１０…生成検査処理部、１０１１…存在検査処理部、１０１２…改竄検知情報生成処理部、１０１３…改竄検知処理部、１１０１…ＣＰＵ、１１０２…メモリ、１１０３…磁気ディスク装置、１１０４…入力装置、１１０５…出力装置、１１０６…ＣＤ－ＲＯＭ装置、１１１０…改竄検知情報生成処理部、１１１１…改竄検知処理部。

【書類名】　　図面

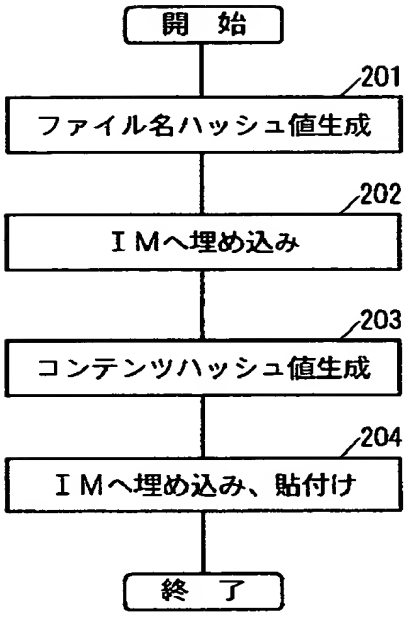
【図１】

図１


100
サーバ装置
101
ＣＰＵ
104
入力装置
105
出力装置
106
CD-ROM
装置
102
メモリ
103
磁気ディスク装置
110
ＩＭ生成処理部
111
改竄検知情報生成処理部
112
改竄検知処理部
WWWサーバ
コンテンツ
コンテンツ
コンテンツ
データ
107
108
Internet
Marks
120
クライアント装置
WWW
ブラウザ

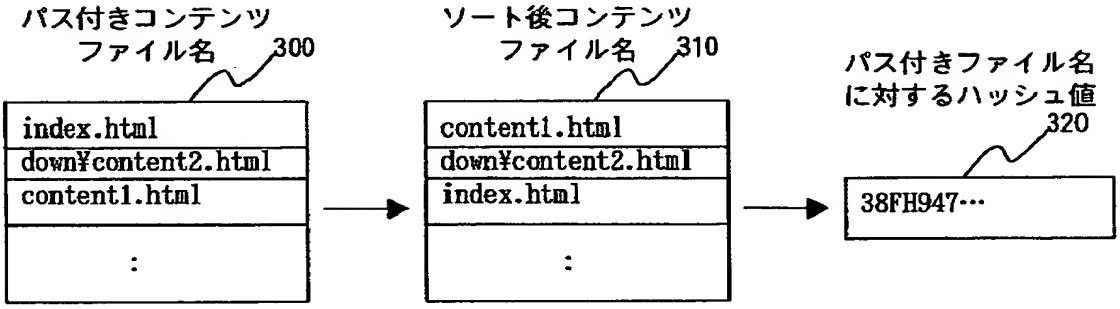
【図２】

図２


開　始
201
ファイル名ハッシュ値生成
202
ＩＭへ埋め込み
203
コンテンツハッシュ値生成
204
ＩＭへ埋め込み、貼付け
終　了

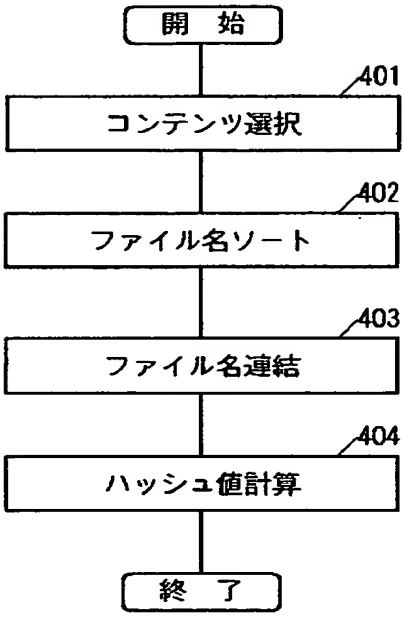
【図３】

図３


パス付きコンテンツ
ファイル名
300
index.html
down¥content2.html
content1.html
:
ソート後コンテンツ
ファイル名
310
content1.html
down¥content2.html
index.html
:
パス付きファイル名
に対するハッシュ値
320
38FH947…

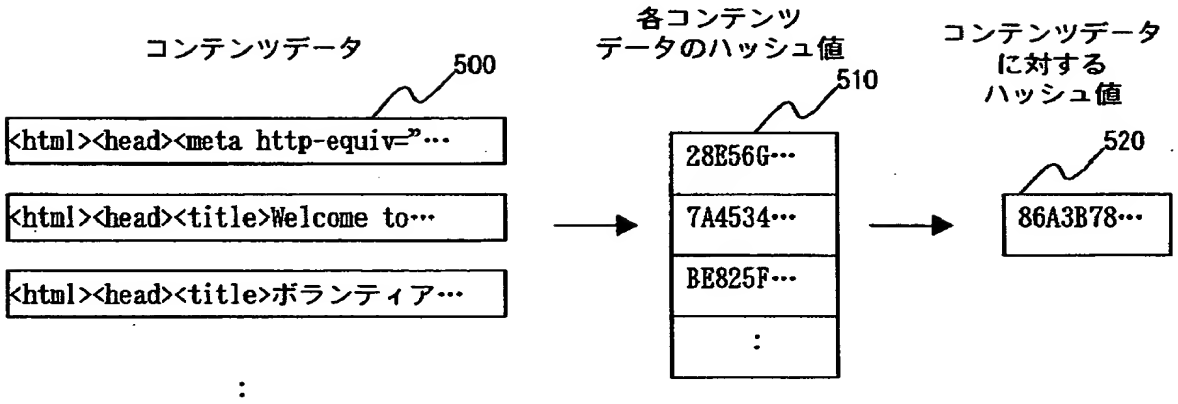
【図４】

図４


開　始
401
コンテンツ選択
402
ファイル名ソート
403
ファイル名連結
404
ハッシュ値計算
終　了

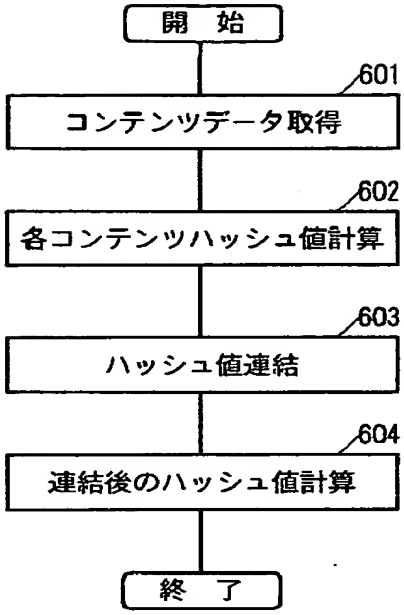
【図５】

図５


コンテンツデータ
500
<html><head><meta http-equiv="…
<html><head><title>Welcome to…
<html><head><title>ボランティア…
:
各コンテンツ
データのハッシュ値
510
28E56G…
7A4534…
BE825F…
:
コンテンツデータ
に対する
ハッシュ値
520
86A3B78…

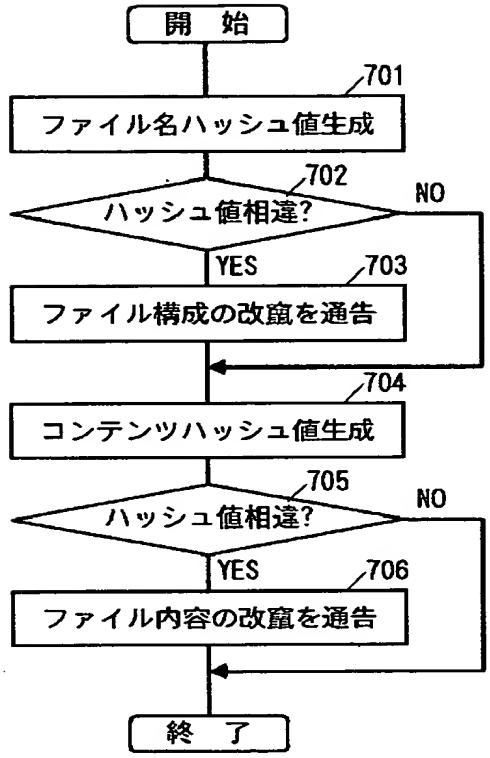
【図６】

図６


開　始
601
コンテンツデータ取得
602
各コンテンツハッシュ値計算
603
ハッシュ値連結
604
連結後のハッシュ値計算
終　了

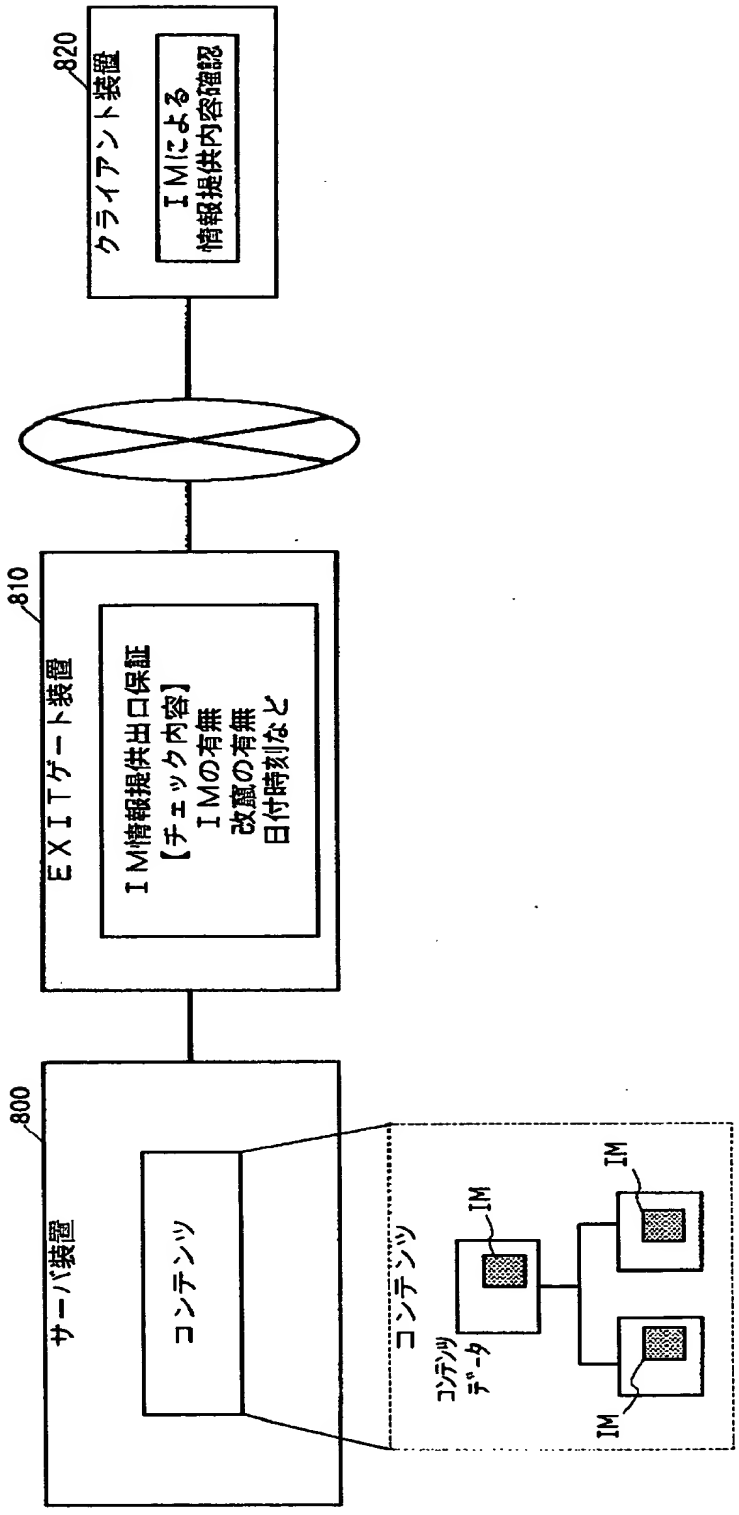
【図７】

図７


開　始
701
ファイル名ハッシュ値生成
702
ハッシュ値相違?
NO
YES
703
ファイル構成の改竄を通告
704
コンテンツハッシュ値生成
705
ハッシュ値相違?
NO
YES
706
ファイル内容の改竄を通告
終　了

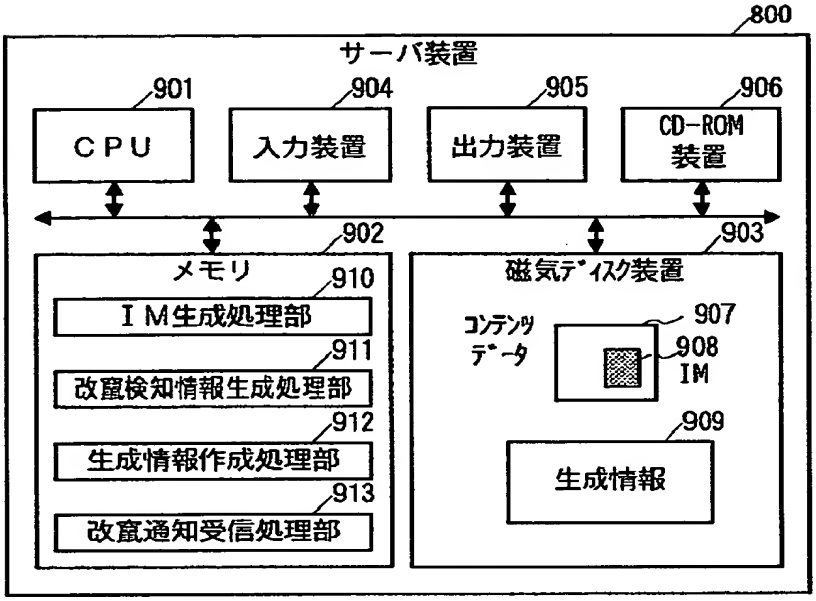
【図８】

図８


820
クライアント装置
ＩＭによる
情報提供内容確認
810
ＥＸＩＴゲート装置
ＩＭ情報提供出口保証
【チェック内容】
ＩＭの有無
改竄の有無
日付時刻など
800
サーバ装置
コンテンツ
コンテンツ
コンテンツ
データ
IM
IM
IM

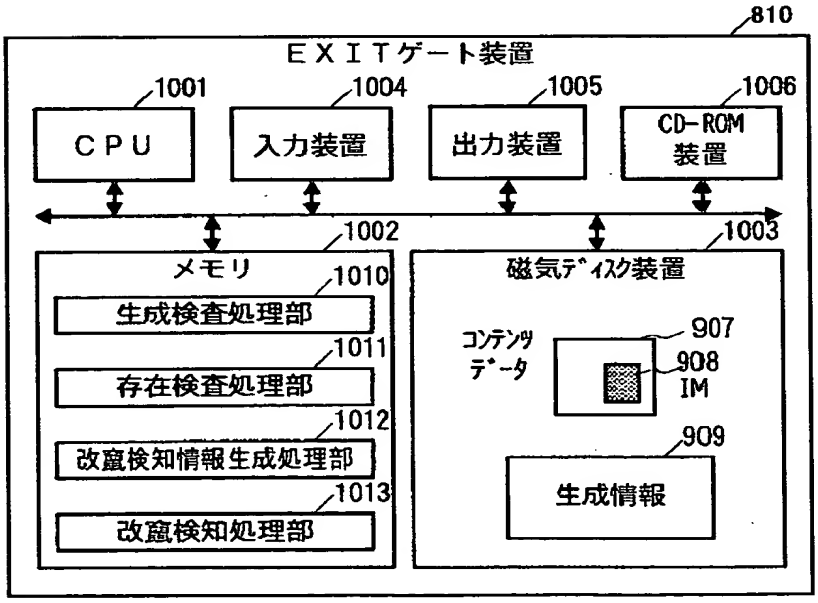
【図９】

図９


800
サーバ装置
901
CPU
904
入力装置
905
出力装置
906
CD-ROM
装置
902
メモリ
910
ＩＭ生成処理部
911
改竄検知情報生成処理部
912
生成情報作成処理部
913
改竄通知受信処理部
903
磁気ﾃﾞｨｽｸ装置
ｺﾝﾃﾝﾂ
ﾃﾞｰﾀ
907
908
IM
909
生成情報

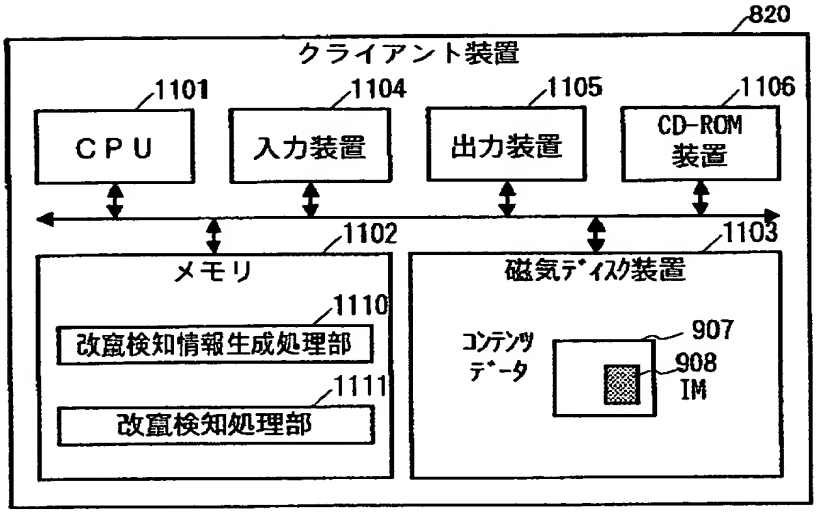
【図１０】

図１０


810
ＥＸＩＴゲート装置
1001
CPU
1004
入力装置
1005
出力装置
1006
CD-ROM
装置
1002
メモリ
1010
生成検査処理部
1011
存在検査処理部
1012
改竄検知情報生成処理部
1013
改竄検知処理部
1003
磁気ﾃﾞｨｽｸ装置
ｺﾝﾃﾝﾂ
ﾃﾞｰﾀ
907
908
IM
909
生成情報

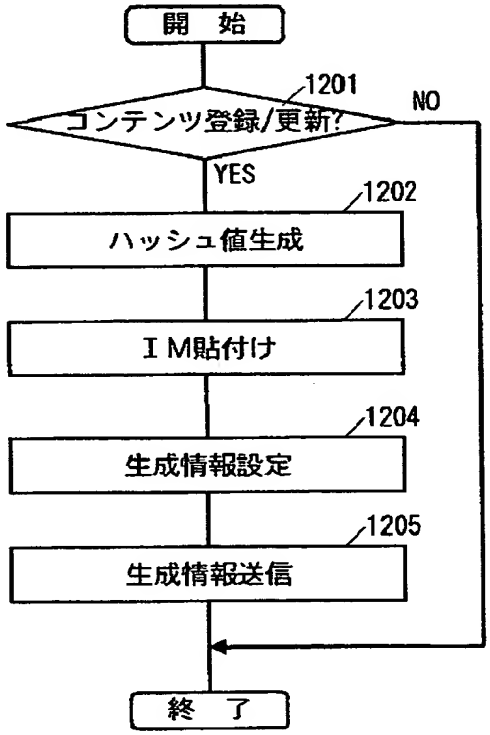
【図１１】

図１１




【図１２】

図１２



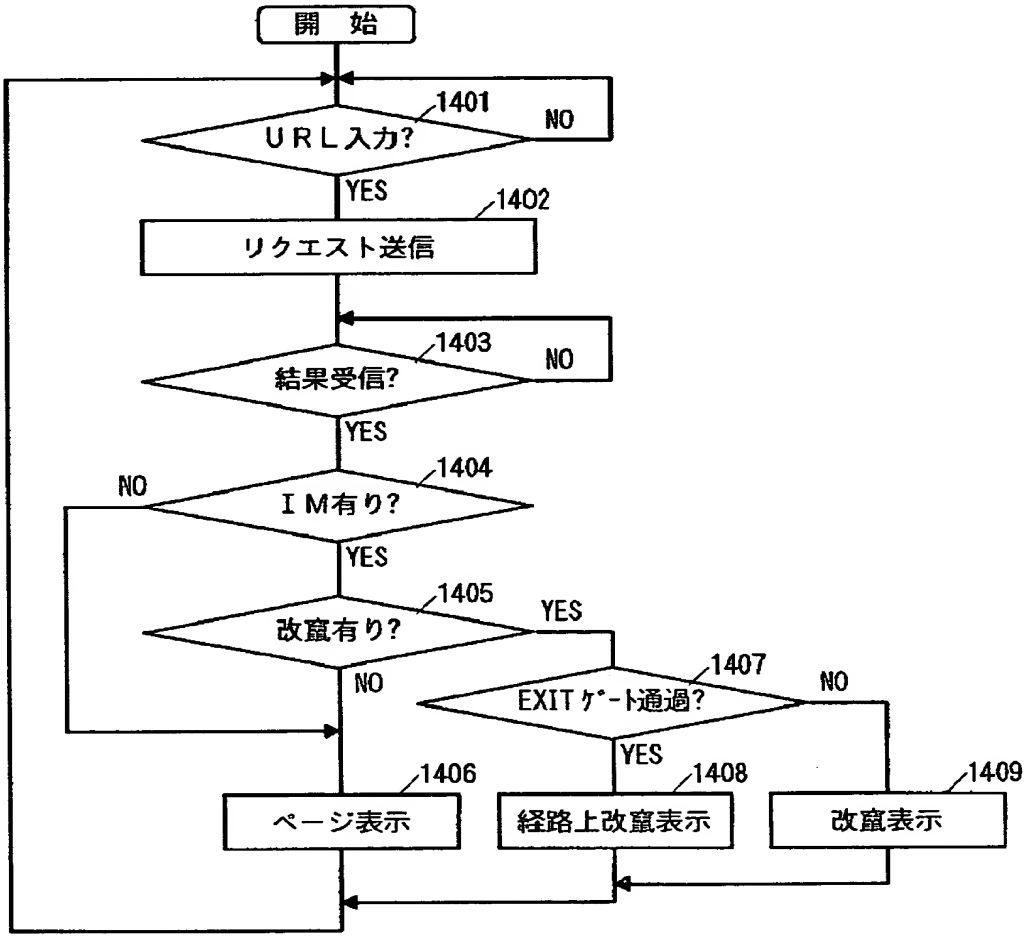
【図１３】

図１３

| ファイル名 | 日付時刻 | … |
|---|---|---|
| index.html | 2000/3/26 11:06 | … |
| down¥content2.html | 2000/3/26 11:16 | … |
| : | : | … |

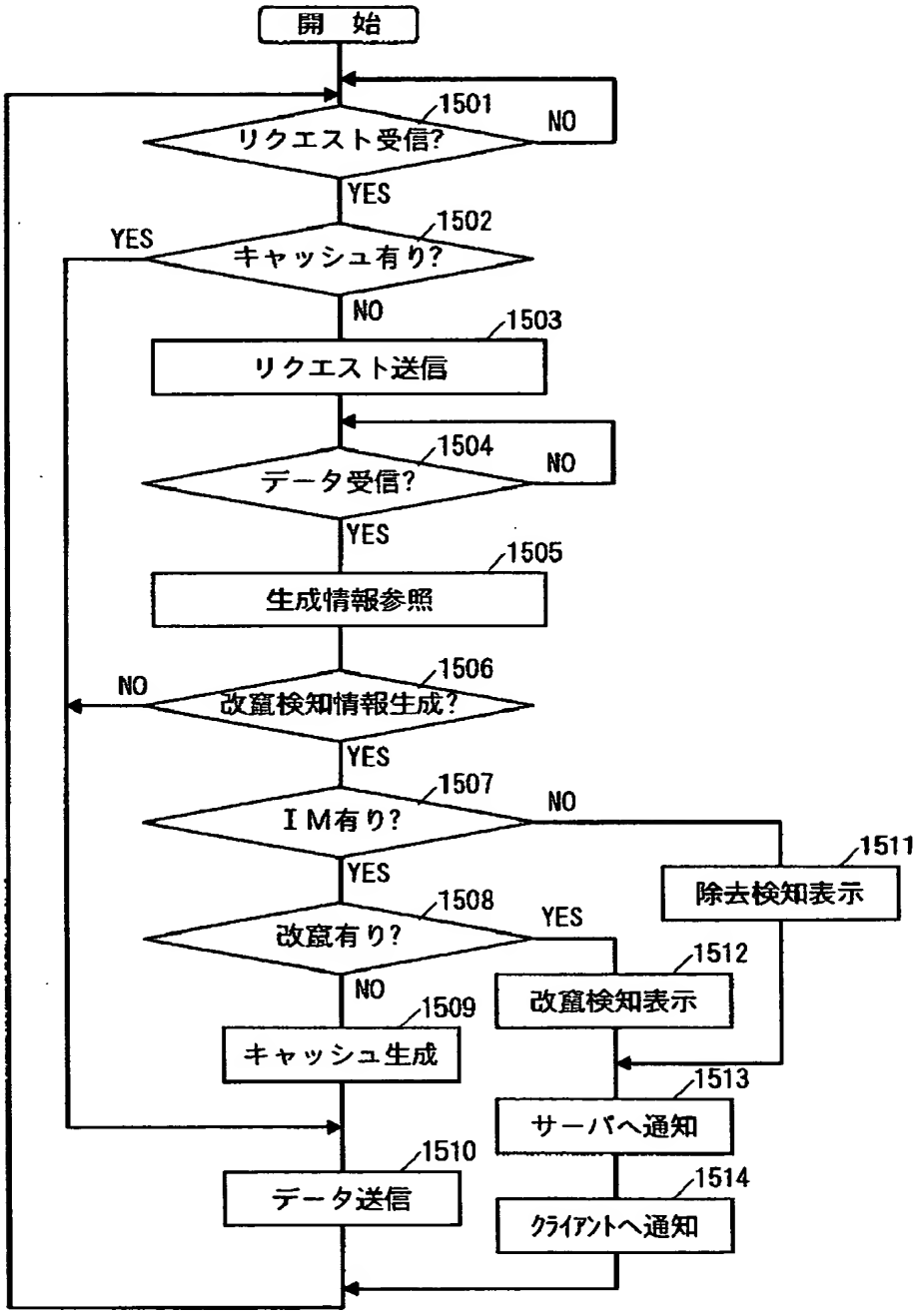
【図１４】

図１４



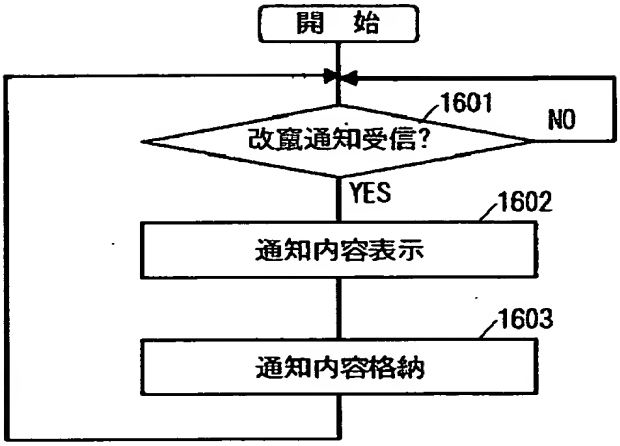
【図１５】

図１５


開　始
1501
リクエスト受信?
NO
YES
1502
キャッシュ有り?
YES
NO
1503
リクエスト送信
1504
データ受信?
NO
YES
1505
生成情報参照
1506
改竄検知情報生成?
NO
YES
1507
ＩＭ有り?
NO
YES
1508
改竄有り?
YES
NO
1509
キャッシュ生成
1510
データ送信
1511
除去検知表示
1512
改竄検知表示
1513
サーバへ通知
1514
ｸﾗｲｱﾝﾄへ通知

【図１６】

図１６



【書類名】　　要約書

【要約】

【課題】　コンテンツの改竄を早期発見することが可能な技術を提供する。

【解決手段】　コンテンツの改竄を検知するコンテンツ改竄検知方法において、複数のコンテンツの現在の構成または内容に対応する改竄検知情報を生成するステップと、当該コンテンツの登録または更新時の構成または内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知するステップとを有するものである。

【選択図】　　図１

# 出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所